

RO/KR 07. 05. 2004



REC'D 25 MAY 2004

WIPO

PCT

별첨 사본은 아래 출원의 원본과 동일함을 증명함

This is to certify that the following application annexed hereto
is a true copy from the records of the Korean Intellectual
Property Office.

출원 번호 : 10-2003-0052939
Application Number

출원 년 월 일 : 2003년 07월 31일
Date of Application JUL 31, 2003

출원 인 : 넥스비(주)
Applicant(s) Nexvi corporation

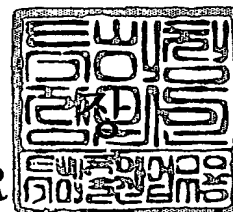
PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)



2004 년 05 월 07 일

특 허 청

COMMISSIONER



【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【참조번호】	0001
【제출일자】	2003.07.31
【국제특허분류】	G09C
【발명의 명칭】	옛보기를 통한 정보유출을 방지하는 비공개 정보입력시스템
【발명의 영문명칭】	PRIVATE INFORMATION INPUTTING SYSTEM PREVENTING INFORMATION OUTFLOW VIA PEEPEING
【출원인】	
【명칭】	넥스비 (주)
【출원인코드】	1-2002-048225-1
【대리인】	
【성명】	이기성
【대리인코드】	9-1999-000252-4
【포괄위임등록번호】	2003-033859-3
【대리인】	
【성명】	김중호
【대리인코드】	9-1998-000638-6
【포괄위임등록번호】	2003-033860-6
【발명자】	
【성명의 국문표기】	김준식
【성명의 영문표기】	KIM, Jun Sik
【주민등록번호】	680322-1069419
【우편번호】	302-122
【주소】	대전광역시 서구 둔산2동 908-1 꿈나무아파트 205-704
【국적】	KR
【발명자】	
【성명의 국문표기】	임상빈
【성명의 영문표기】	YIM, Sang Bin
【주민등록번호】	720328-1524618

【우편번호】 302-809
 【주소】 대전광역시 서구 갈마2동 1066-301
 【국적】 KR

【발명자】

【성명의 국문표기】 김병성
 【성명의 영문표기】 KIM, Byung Sung
 【주민등록번호】 780812-1403414
 【우편번호】 300-802
 【주소】 대전광역시 동구 가양2동 160-45
 【국적】 KR

【우선권주장】

【출원국명】 KR
 【출원종류】 특허
 【출원번호】 10-2003-0023529
 【출원일자】 2003.04.14
 【증명서류】 미첨부

【우선권주장】

【출원국명】 KR
 【출원종류】 특허
 【출원번호】 10-2003-0030425
 【출원일자】 2003.07.04
 【증명서류】 미첨부

【심사청구】

청구

【취지】

특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의
 한 출원심사를 청구합니다. 대리인
 이기성 (인) 대리인
 김중호 (인)

【수수료】

【기본출원료】	20	면	29,000	원
【가산출원료】	25	면	25,000	원
【우선권주장료】	2	건	43,000	원
【심사청구료】	13	항	525,000	원

【합계】	622,000 원
【감면사유】	소기업 (70%감면)
【감면후 수수료】	216,700 원
【첨부서류】	1. 요약서·명세서(도면)_1통 2.소기업임을 증명하는 서류[상시종 업원수확인서류는 신고설립기업임 으로 생략됨]_1통

【요약서】**【요약】**

옛보기를 통한 정보 유출을 방지하는 비공개 정보 입력 시스템이 개시된다. 키 영상을 생성하는 수단과, 상기 키 영상을 마스킹하는 마스킹 영상을 생성하는 수단과, 상기 키 영상과 상기 마스킹 영상에 대한 영상 시퀀스를 생성하는 수단과, 상기 영상 시퀀스에 따라 상기 키 영상과 상기 마스킹 영상을 디스플레이하는 키 표시부와, 상기 키 표시부에 의해 디스플레이되는 키 영상의 소정 위치에서 상응하는 키의 정보를 입력받는 키 입력부와, 상기 키 입력부를 통해 입력된 정보를 상기 키 영상에 따라 실제 키 값으로 변환하는 비공개 입력 장치 제어수단을 포함한다. 셔터부와, 상기 영상 시퀀스에 상응하는 셔터 개폐 시퀀스에 따라 상기 셔터부를 개폐하는 셔터 제어부를 구비하는 셔터 개폐 수단을 더 포함한다.

【대표도】

도 2

【명세서】

【발명의 명칭】

엿보기를 통한 정보 유출을 방지하는 비공개 정보 입력 시스템{PRIVATE INFORMATION INPUTTING SYSTEM PREVENTING INFORMATION OUTFLOW VIA PEEPEING}

【도면의 간단한 설명】

도 1a 및 도 1b는 본 발명에 따른 비공개 정보 입력 시스템의 기본 구성도.

도 2는 키 디스플레이로서 전용 디스플레이를 사용하는 제1 실시예의 제어 구성도.

도 3은 키 디스플레이로서 범용 모니터를 사용하고 범용 컴퓨터로 제어를 수행하는 제2 실시예의 제어 구성도.

도 4는 전용 드라이버를 사용하는 제3 실시예의 제어 구성도.

도 5는 본 발명에 따른 비공개 정보 입력 시스템의 작동 순서도.

도 6은 본 발명에 따른 키패드 배치 방법을 설명하는 도면.

도 7은 본 발명에 따른 완성형 혼합 영상을 설명하는 도면.

도 8은 본 발명에 따른 유사 완성형 혼합 영상을 설명하는 도면.

도 9는 본 발명에 따른 완성형 혼합 영상을 이용한 영상 배합 규칙, 영상 시퀀스, 셔터 개폐 시퀀스 선정을 설명하는 도면.

도 10은 본 발명에 따른 완성형 혼합 영상을 이용한 요소 영상법을 설명하는 도면.

도 11은 본 발명에 따른 동일 손동작 키 관리 방법을 설명하는 도면.

도 12는 본 발명에 따른 동일 손동작 키 관리 방법의 순서도.

【발명의 상세한 설명】**【발명의 목적】****【발명이 속하는 기술분야 및 그 분야의 종래기술】**

- <13> 본 발명은 엿보기를 통한 정보 유출을 방지하는 비공개 정보 입력 시스템에 관한 것이다.
- <14> 점포, 은행 등에서 각종 카드를 사용하거나, 텔레뱅킹, 인터넷뱅킹 등의 금융거래를 할 때 비밀번호 및 개인정보 유출로 인한 금융 사고가 빈번하게 발생하고 있다. 따라서 고객이 비밀번호를 안전하게 사용하고 개인정보 및 거래정보를 안전하게 처리하도록 하기 위한 다각도의 대책이 수립되고 있다. 출금표에서 비밀번호 기재란을 삭제하고 출금할 때나 신용카드를 결제할 때 비밀번호 입력기를 이용하는 방안과, 고객의 개인정보와 거래정보를 암호화하여 저장하고 접근을 제어함으로써 은행 내부자에 의하여 고객 정보가 유출되는 것을 방지하는 방안이 추진되고 있다. 또한 네트워크 해킹을 통한 정보 유출은 수 많은 관련 보안 업체들의 노력으로 효과적으로 차단되고 있다.
- <15> 그렇지만 고객은 정보 입력 과정에서 비밀번호 및 개인정보의 물리적인 노출에 여전히 무방비 상태로 놓여 있다. 사용자가 현금자동지급기(cash dispenser: CD), 현금자동입출금기(automated teller machine: ATM), 비밀번호입력기(PIN pad)의 키패드(key pad)에서 비밀번호 및 개인정보를 입력할 때, 비밀번호 및 개인정보는 사용자가 키패드에서 키(key)를 입력하는 동안 입력중인 키나 손동작을 주위에서 엿보거나, 키에 남겨진 지문 조사, 키를 누를 때 나는 소리 청취 등의 물리적인 방법을 통해 유출될 수 있다. 나아가 몰래카메라 촬영과 망원경을 통한 엿보기도 세계적으로 확산되고 있다.

<16> 이러한 물리적인 비밀번호 및 개인정보 유출로 인한 피해가 상당하지만, 이러한 피해가 발생하면 금융기관들은 비밀번호 관리를 소홀히 했다는 이유로 고객에게 모든 책임을 전가하는 실정이다. 기존의 키패드를 계속 사용한다면, 고객정보 암호화 저장과 해킹 방지에 대한 관리가 강화될수록 향후에는 상대적으로 보안이 취약한 엿보기를 통한 정보 유출을 비롯한 물리적인 정보 유출이 더욱더 심해질 전망이다.

<17> 금융거래 뿐만 아니라 한편, 휴대폰, PDA, 노트북 등과 같은 휴대용 컴퓨터의 발전과 데스크탑 PC, CD, ATM, 키오스크(kiosk), 판매시점관리(point of sale: POS) 단말기, 사무실 및 아파트 출입문의 도어록(door lock)과 같은 디지털 출입장치, 키입력방식 귀중품보관장치 등의 광범위한 보급으로 인하여 공개 장소에서 더욱더 많은 정보기기들이 사용되고 있다. 이 때, 이러한 정보기기의 디스플레이 모니터의 내용과 사용자가 정보기기에 정보 입력을 하는 과정은 그 정보기기의 가시거리 내에 있는 불특정한 사람이 볼 수 있는 가능성이 있다. 특히 사용자가 정보기기에서 디스플레이되는 정보를 일반적으로 시청할 때 보다는 사용자가 정보 입력을 하는 과정이 보안상 더욱 중요하다. 정보 입력과정에서는 많은 경우 개인정보, 거래정보, 기밀정보와 같은 중요한 정보를 입력하고 처리해야 하므로 입력정보의 엿보기를 통한 정보 유출을 비롯한 물리적 유출의 방지가 중요해진다.

<18> 도둑, 스파이, 프라이버시 침해 범죄자와 같은 악의적인 엿탐자(peeper)는 사용자가 정보를 입력하는 순간을 특별히 주시한다. 엿탐자는 사용자의 모니터나 키패드 엿보기를 통해 엿탐하거나 사용자가 정보를 입력하는 손동작 및 몸동작 등을 엿보아 정보를 엿탐한다. 숙련된 엿탐자는 잠깐의 모니터, 키패드 엿보기나 손동작 및 몸동작 엿탐을 통해 상당히 높은 정확도로 사용자의 입력정보를 해독할 가능성이 있다. 아울러 사용자가 이용을 끝낸 후 정보기기를

떠났을 때 염탐자는 키패드 위에 있는 손자국이나 지문, 키패드 마모 등의 입력 흔적을 채취하여 사용자의 입력정보를 해독할 가능성도 있다.

- <19> 종래에는 입력정보의 시각 보안을 위한 적당한 방법이 없었기 때문에 정보 입력과정에서 주위에 염탐자가 있는 지에 대한 사용자의 주의가 각별히 요구되었다.
- <20> 최근에는 생체인식기술을 도입하여 아이디와 비밀번호를 사용하지 않고 사용자 인증을 하는 사례가 있다. 그러나 생체인식만으로 사용자 인증을 하는 것은 기술적인 미비성과 예기치 못한 생체인식기 오작동, 상해로 인한 지문 등의 생체정보의 훼손과 같은 문제점이 있다. 또한 프라이버시 침해 가능성이 존재하기 때문에 광범위하게 적용되기 어렵다. 일반적으로 인증 방법은 기본적으로 '사용자 생체정보', '사용자가 갖고 있는 것', '사용자가 알고 있는 것'의 조합을 사용하기 때문에 신상정보 및 비밀번호를 입력해야 하는 경우가 많다. 게다가 생체인식만으로 사용자 인증을 하더라도 거래정보 등을 기입해야 할 필요성을 제거하지는 못한다. 상기와 같이 생체인식기술로는 정보 입력과정에서 시각 보안을 제대로 실현할 수 없다.
- <21> 정보 입력시스템의 시각 보안을 위한 종래 기술로는 키패드의 자판 배치를 가변하는 방법과 장치가 있다. 전통적인 키패드는 자판의 배치가 정해져 있는 형태를 띄고 있다. 이를 개선한 방법으로서 사용자가 기밀정보를 입력하려고 할 때 자판을 가변하여 배치하고 입력하면 엿보기를 일정정도 방지할 수 있다. 이러한 목적을 위한 자판 배치 관련 특허는 한국특허출원 1999-0012741(출원인은 "이상열", 발명의 명칭은 "키입력 장치"임)과 미국특허 제4,857,914호(발명자는 "Thrower"임) 등이 있다.
- <22> 그러나 키패드의 자판 배치를 가변하는 입력 방법은 염탐자가 사용자의 정보 입력과정에서 키패드의 자판 배치를 엿보지 못하고 손동작 엿보기만 가능할 경우에 효과적인 방법으로서,

염탐자가 사용자 뒤에서 어깨 너머로 또는 사용자 주위에서 키패드의 자판 배치와 입력키를 맨 눈이나 망원경, 카메라 촬영을 통하여 엿보게 되면 그대로 정보 유출이 가능하게 되는 매우 불완전한 방법이다.

<23> 정보 입력시스템의 시각 보안을 위한 기술은 아니지만 연관 기술로서, 비공개 디스플레이가 미국특허 제5,629,984호(출원인은 "선마이크로시스템즈"임), 한국특허출원 2003-3600(출원인은 "넥스비"임)과 한국특허출원 2003-9274(출원인은 "넥스비"임)에 개시되어 있다. 비공개 디스플레이는 공개적으로 볼 수 있는 모니터 상에서 허가된 사용자에게 비공개 정보를 제공하고, 반면에 권한이 부여되지 않은 사람은 동일한 모니터 상의 비공개 정보를 볼 수 없는 디스플레이이다.

<24> 그러나 비공개 디스플레이는 모니터의 시각 보안에만 초점을 맞추고 있고 정보 입력 행위 과정에서의 보안에는 적합하지 않다. 시각 보안을 위해 비공개 디스플레이를 이용해도 키패드로 정보를 입력할 때 염탐자가 키패드 자판이나 손동작을 엿보아 해독하는 것을 방지하지는 못한다. 또한 키패드 위에 있는 손자국이나 지문 등의 입력 흔적을 채취하여 사용자의 입력정보를 해독하는 것을 방지하지는 못한다. 이와 같이 비공개 디스플레이는 사용자의 정보 입력 행위 과정에 대한 총체적인 보안에는 미흡한 실정이다.

【발명이 이루고자 하는 기술적 과제】

<25> 본 발명은 이러한 종래기술의 문제점을 해결하기 위하여 제안된 것으로서, 비공개 디스플레이의 기본 개념을 정보 입력 장치로 확장하고 사용자의 정보 입력 행위 과정을 총체적인 물리적 보안 측면에서 고려하여 안전한 비공개 정보 입력 장치를 제공하는 것을 일 목적으로 한다.

- 26> 본 발명은 사용자가 정보 입력을 할 때의 키패드의 자판 배치와 입력키를 염탐자가 엿보아 해독하는 것을 방지하는 비공개 정보 입력 장치를 제공하는 것을 다른 목적으로 한다.
- 27> 본 발명은 사용자가 정보 입력을 할 때의 손동작을 염탐자가 엿보아 해독하는 것을 방지하는 비공개 정보 입력 장치 및 방법을 제공하는 것을 또 다른 목적으로 한다.
- 28> 본 발명은 키패드 등의 키입력 수단 위에 있는 손자국이나 지문, 키패드 마모 등의 입력 흔적을 염탐자가 채취하여 사용자의 입력정보를 해독하는 것을 방지하는 비공개 정보 입력 장치를 제공하는 것을 또 다른 목적으로 한다.
- 29> 본 발명은 비공개 정보 입력 시스템에 적합한 마스킹 영상을 생성하는 장치를 제공하는 것을 또 다른 목적으로 한다.
- 30> 본 발명은 염탐자가 동일한 종류의 다른 서터 개폐 수단 등의 필터 수단을 가지고 엿보려 해도 정보 입력 내용을 알아챌 수 없도록 하는 비공개 정보 입력 장치를 제공하는 것을 또 다른 목적으로 한다.

【발명의 구성】

- 31> 전술한 바와 같은 목적을 달성하기 위한 본 발명은 엿보기를 통한 정보 유출을 방지하는 비공개 정보 입력 시스템에 있어서, 키 영상을 생성하는 수단과, 상기 키 영상을 마스킹하는 마스킹 영상을 생성하는 수단과, 상기 키 영상과 상기 마스킹 영상에 대한 영상 시퀀스를 생성하는 수단과, 상기 영상 시퀀스에 따라 상기 키 영상과 상기 마스킹 영상을 디스플레이하는 키 표시부와, 상기 키 표시부에 의해 디스플레이되는 키 영상의 소정 위치에서 상응하는 키의 정보를 입력받는 키 입력부와, 상기 키 입력부를 통해 입력된 정보를 상기 키 영상에 따라 실제 키 값으로 변환하는 비공개 입력 장치 제어수단을 포함한다. 서터부와, 상기 영상 시퀀스에 상

응하는 셔터 개폐 시퀀스에 따라 상기 셔터부를 개폐하는 셔터 제어부를 구비하는 셔터 개폐 수단을 더 포함한다.

<32> 이러한 본 발명에 의하여 사용자의 정보 입력 행위 과정을 총체적인 물리적 보안 측면에서 고려하여 안전한 비공개 정보 입력 장치 및 방법을 제공할 수 있다. 또한 사용자가 정보 입력을 할 때의 키패드의 자판 배치와 입력키를 염탐자가 엿보아 해독하는 것을 방지할 수 있다. 또한 사용자가 정보 입력을 할 때의 손동작을 염탐자가 엿보아 해독하는 것을 방지할 수 있다. 또한 키입력 수단 위에 있는 손자국이나 지문, 키패드 마모 등의 입력 흔적을 염탐자가 채취하여 사용자의 입력정보를 해독하는 것을 방지할 수 있다. 또한 비공개 정보 입력 시스템에 적합한 마스킹 영상을 생성할 수 있다. 또한 염탐자가 동일한 종류의 다른 셔터 개폐 수단을 가지고 엿보려 해도 정보 입력 내용을 알아챌 수 없도록 하는 비공개 정보 입력 장치 및 방법을 제공할 수 있다.

<33> 이하, 첨부된 도면을 참조하여 본 발명의 실시예들을 상세히 설명한다. 설명의 편의상 도면에서 동일한 참조부호는 동일 또는 유사한 구성요소 또는 신호를 가리키는 것으로 사용된다.

<34> 먼저 도 1a 및 도 1b는 본 발명에 따른 비공개 정보 입력 시스템의 기본 구성도이다. 도 1a에 도시되어 있는 바와 같이, 비공개 입력 장치(100)는 입력 장치 제어 시스템(102), 키(key) 디스플레이(104), 키패드 입력 수단(106), 필터 역할을 하는 셔터 개폐 수단(108), 입력 장치 제어 시스템(102)과 셔터 개폐 수단(108)을 연결하는 유무선 통신수단(110), 호스트 컴퓨터가 있는 경우 호스트 컴퓨터(도시되지 않음)와 상기 입력 장치 제어 시스템(102)을 연결하는 유무선 통신수단(도시되지 않음)으로 구성된다.

- <35> 입력 장치 제어 시스템(102)은 사용자의 요구에 의하거나 자체적으로 숫자키 또는 문자키의 비공개 영상과, 비공개 영상을 마스킹하는 마스킹 영상을 영상 시퀀스에 따라 시간 순차적으로(time-sequentially) 교체하면서 키 디스플레이(104)에 디스플레이하고, 상응하는 셔터 개폐 신호를 셔터 개폐 수단(108)에 전송하여 셔터 개폐 수단(108)을 작동함으로써 허가된 사용자만이 비공개로 정확한 숫자키 또는 문자키를 볼 수 있도록 한다.
- <36> 키 디스플레이(104)는 일반적인 LCD, CRT, EL 디스플레이 모니터일 수 있다. 이 경우는 모니터에 숫자키 또는 문자키를 디스플레이하여 구현된다. 다른 실시예에서, 키 디스플레이(104)는 LED의 배열로 구성된다. 다른 실시예에서, 키 디스플레이(104)는 도 1a에 도시되어 있는 바와 같이 간단한 7-세그먼트(segment) 발광 다이오드(light-emitting diode : LED)의 배열로 구성된다.
- <37> 키패드 입력 수단(106)은 도 1a에 도시되어 있는 바와 같이 투명한 키패드가 키 디스플레이(104)를 덮은 형태로 설치될 수 있다. 다른 실시예에서는 키 디스플레이(104)의 각각의 키 아래에 키 버튼이 놓여 있는 형태로 구성될 수 있다. 허가된 사용자는 비공개로 키 디스플레이(104)가 디스플레이하는 정확한 숫자키 또는 문자키를 보면서 상응하는 키패드 위에 있는 키를 입력하고, 키패드 입력 수단(106)은 입력된 키 값을 입력 장치 제어 시스템(102)에 전송한다.
- <38> 셔터 개폐 수단(108)은 기계식 또는 액정 셔터와 같은 광전식일 수 있다. 셔터 개폐 수단(108)은 셔터 렌즈를 한 개 또는 여러 개를 가진 셔터 안경, 평면 셔터 패널, 지지대를 가진 셔터 구조물, 셔터 모자와 같이 다양한 형태로 제작될 수 있다. 도 1a에는 평면 패널 형태의 셔터 개폐 수단을 도시하고 있다.

- <39> 비공개 정보 입력 장치를 주위가 밝은 곳에서 사용할 경우에는 키 디스플레이(104)에서 반사된 주변광이 사용자 눈에 입사하여 영상의 대비(contrast)가 낮아지는 문제가 발생할 수 있다. 일 실시예에서는 3M사가 판매하고 있는 "3M™ Privacy Computer Filters"와 같은 주변광 차단 필터(도시되지 않음)를 키 디스플레이(104)의 전면면에 부착한다. 주변광 차단 필터는 광투과율이 입사각에 의존하는 광필터로서 입사각이 특정 각도 이상인 광을 차단하는 필터이다. 다른 실시예에서는 셔터 개폐 수단(108)으로 직접 입사하는 주변광을 차단하기 위하여 상기 주변광 차단 필터를 셔터 개폐 수단(108)에 부착한다.
- <40> 셔터 개폐 수단(108)은 사용 감지 수단(도시되지 않음)을 더 포함하여 구성될 수 있다. 사용 감지 수단은 사용자가 셔터 개폐 수단(108)을 사용하려는 의도를 감지하여 입력 장치 제어 시스템(102)에 전달하여 적절한 대응을 하도록 한다. 사용 감지 수단은 셔터 개폐 수단(108)의 손잡이에서 접촉 센서, 전기 센서, 광센서 등으로 구현되어 사용자의 손의 접촉 여부나 셔터 개폐 수단(108)의 이동 여부를 감지한다. 다른 예로서 유무선 통신수단(110)에서 센서로 구현되어 셔터 개폐 수단(108)의 이동을 감지한다. 다른 예로서 셔터 개폐 수단(108)을 놓는 접촉부나 장착부가 존재하여 사용자가 셔터 개폐 수단(108)을 들어 올릴 때와 놓을 때를 접촉부나 장착부가 감지한다.
- <41> 도 1b는 비공개 키패드 입력 장치의 작동 화면이다. 7-세그먼트 LED를 이용한 도 1b의 실시예에서는 맨눈으로 보는 사람은 키패드 입력 장치의 모든 키가 숫자 '8'로 보인다. 셔터 개폐 수단(108)을 통해 보는 허가된 사용자만이 정확한 키 값을 보면서 정보를 입력할 수 있다. 사용자가 정보를 입력할 때 키패드의 키 배치를 다양한 방법으로 변화시키면 엿보기에 의한 입력정보 유출을 원천적으로 차단한다.

- <42> 본 명세서에서 모니터의 수직동기(vertical sync)로 구별되는 하나의 디스플레이 화면을 모니터 프레임(monitor frame)이라 하고, 영상 데이터의 한 조각을 영상 데이터 프레임(image data frame)이라 한다. 하나의 영상 데이터 프레임은 모니터의 한 프레임과 같은 크기일 수도 있고 다를 수도 있다. 비공개 영상(private image : 이하, "P 영상"이라고 함)은 허가된 사용자의 사적인 비공개 영상이다. 마스킹 영상(masking image : 이하, "M 영상"이라고 함)은 비허가자가 허가된 사용자의 비공개 영상을 보지 못하도록 차단하는 영상이다.
- <43> 도 2는 키 디스플레이로서 전용 디스플레이를 사용하는 제1 실시예의 제어 구성도이다. 도 2에서는 키 디스플레이로서 LED 배열이나 7-세그먼트 LED와 같은 간단한 전용 디스플레이를 사용하고 비공개 키패드 입력 장치의 제어는 전용 제어 시스템으로 행한다.
- <44> 비공개 입력 장치 제어 수단(202)은 보안 성능 제어부, 영상 배합 규칙 선정부, 암호화부, 관리부로 이루어지며, 디스플레이 보안 수준을 기준으로 영상 시퀀스 생성 수단(212), 셔터 개폐 시퀀스 및 셔터 개폐 신호 생성 수단(214), 비공개 영상 및 마스킹 영상 생성 수단(216)을 제어한다. 다른 실시예에서는 비공개 입력 장치 제어 수단(202)은 사용자 인증부를 더 포함하며, 사용자를 인증하고 허가된 사용자의 인증 수준에 맞추어 디스플레이 보안 수준을 설정하고 관리한다. 사용자 인증 방법은 사용자의 식별부호(identification number : 이하, "ID"라고 함)와 비밀번호 입력을 받아 인증할 수 있다. 또한 허가된 셔터 개폐 수단(108)을 연결함으로써 사용자 인증을 할 수 있다. 허가된 셔터 개폐 수단 여부 인증은 셔터 개폐 수단(108)의 판독 전용 메모리(read only memory : ROM)(도시되지 않음)에 내장된 제품의 일련번호 등으로 수행한다.
- <45> 디스플레이 보안 수준은 디폴트로 설정될 수 있고 오퍼레이터가 호스트 컴퓨터(240)의 오퍼레이터 인터페이스(246)에서 설정하던지 사용자가 키패드 입력 장치에서 직접 설정할 수

있다. 디스플레이 보안 수준은 '사용자 시지각 성능', '맨눈 보안 성능', '염탐자 대항 보안 성능' 등 세가지 영역에서 요구하는 성능의 수준에 따라 결정된다. '사용자 시지각 성능'은 허가된 사용자가 영상을 시각적 불편 또는 피로감 없이 명료하게 볼 수 있도록 하는 것이고, '맨눈 보안 성능'은 셔터를 갖지 않은 비허가자가 영상을 명료하게 볼 수 없도록 하는 것이며, '염탐자 대항 보안 성능'은 셔터를 가진 비허가자나 염탐자(peeper)가 영상을 명료하게 볼 수 없도록 하는 것이다.

<46> 보안 성능 제어부는 디스플레이 보안 수준 정보를 입력 받아 영상 배합 규칙 선정부, 영상 시퀀스 생성 수단(212), 셔터 개폐 시퀀스 및 셔터 개폐 신호 생성 수단(214), 비공개 영상 및 마스킹 영상 생성 수단(216)에 적절한 정보를 생성하여 전송한다. 영상 배합 규칙 선정부는 디스플레이 보안 수준 정보에 따라 배합할 비공개(P) 영상과 마스킹(M) 영상의 종류 선택, P/M 영상의 평균 배합 비율 선정, 평균 배합 비율을 유지하면서 영상 시퀀스를 생성하기 위한 P/M 영상 시퀀스 생성 방법론 선정 등을 실행한다. 아울러 셔터 개폐 시퀀스 생성 방법론을 선정한다. 중간상태 셔터 개폐를 이용하면 더욱 다양한 영상배합 규칙을 선정할 수 있다.

<47> 다른 실시예에서는 비공개 입력 장치 제어 수단(202)의 영상 배합 규칙 선정 및 관리 기능 중 일부 기능은 호스트 컴퓨터에서 수행할 수 있다.

<48> 영상 시퀀스 생성 수단(212), 셔터 개폐 시퀀스 및 셔터 개폐 신호 생성 수단(214), 비공개 영상 및 마스킹 영상 생성 수단(216)은 사용자의 인증 수준 및 디스플레이 보안 수준에 따라 상응하는 영상 시퀀스, 셔터 개폐 시퀀스 및 셔터 개폐 신호, 비공개 영상 및 마스킹 영상을 각각 생성한다. 셔터 개폐 시퀀스 및 셔터 개폐 신호 생성 수단(214)는 영상 시퀀스에 상응하여 셔터 개폐 시퀀스를 생성하고, 셔터 개폐 시퀀스에 따라 현재 시점의 셔터 개폐 신호를 생성한다. 일 실시예에서는 상기 셔터 개폐 신호는 암호화되어 생성된다.

<49> 시퀀스 제어기(210)는 상기 비공개 입력 장치 제어 수단(202)과 정보를 교환하면서 생성된 영상 시퀀스에 따라 비공개 영상 및 마스킹 영상 생성 수단(216)에서 생성된 비공개 영상인 키 영상 및 키 영상의 마스킹 영상을 키 디스플레이 제어기(204)에 제공한다. 키 디스플레이 제어기(204)는 키 디스플레이(104)에 영상 시퀀스에 따른 비공개 영상인 키 영상 및 키 영상의 마스킹 영상을 디스플레이한다. 또한 시퀀스 제어기(210)는 상기 셔터 개폐 시퀀스 및 셔터 개폐 신호 생성 수단(214)에서 생성된 셔터 개폐 신호를 적절히 제어하여 P-S 송수신부(208)를 통하여 상기 셔터 개폐 수단(108)에 전송한다. 셔터 개폐 신호를 상기 셔터 개폐 수단(108)에 전송하는 유무선 통신수단(110)은 USB, 직렬 링크(serial link)와 같은 유선링크나 IR, RF(FM, AM, Bluetooth)와 같은 무선링크로 구현될 수 있다.

<50> 셔터 개폐 수단(108)은 S-P 송수신부(230)와 디코더/인증수단(232)과 셔터 제어기(234)와 셔터부(236)로 이루어질 수 있다. S-P 송수신부(230)는 P-S 송수신부(208)로부터 전송된 셔터 개폐 신호를 수신하여 디코더/인증수단(232)에 전송한다. 디코더/인증수단(232)은 셔터 개폐 신호를 해독하여 셔터 개폐 시퀀스 상태값을 획득하고, 셔터 제어기(234)는 셔터 개폐 시퀀스 상태값에 따라 셔터부(236)를 완전히 개폐하거나 중간 상태로 개폐한다. 다른 실시예에서는 셔터 개폐 신호를 암호화 없이 전송하고 디코더/인증수단(232)을 생략하고 구현할 수 있다. 또 다른 실시예에서는 셔터 제어기(234)를 입력 장치 제어 시스템(102)에 포함시키고 셔터 제어기(234)와 셔터 개폐 수단(108)의 셔터부(236)를 간단한 직렬 링크 등으로 구성할 수 있다.

<51> 키패드 자판 배치 수단(220)은 키 배치 유형을 결정하고 정해진 키 배치 유형 가운데에서 현재 시점의 키 배치를 결정한다. 이 때 난수 발생기(Random number generator) 등을 사용할 수 있다. 일 실시예에서는 사용자가 키 배치 유형을 선택할 수 있다. 키 배치 유형에는 후술할 쉬프트(shift)배치, 회전 배치, 무작위 배치 유형이 있다. 키패드 자판 배치 수단(220)은

결정된 현재 시점의 키 배치를 비공개 입력 장치 제어 수단(202)에 전송하고, 비공개 입력 장치 제어 수단(202)의 관리하에 시퀀스 제어기(210)와 비공개 영상 및 마스킹 영상 생성 수단(216)이 키 배치에 해당하는 영상을 키 디스플레이 제어기(204)를 통해 키 디스플레이(104)에 디스플레이 한다. 사용자는 키 디스플레이(104)에 디스플레이된 키 배치를 비공개로 보면서 키패드(106)에서 정보를 입력한다. 키패드(106)에서 입력된 키는 키패드 제어기(206)에서 해당하는 위치 키 값으로 판독되고 판독된 위치 키 값이 키패드 자판 배치 수단(220)의 키 배치에 따라 실제 키 값으로 변환된다. 사용자가 입력한 실제 키 값은 비공개 입력 장치 제어 수단(202)의 관리부에서 처리된다. 일 실시예에서는 호스트 컴퓨터(240)가 존재하여 입력된 실제 키 값을 상기 호스트 컴퓨터(240)에 전송하고 호스트 컴퓨터(240)의 관리 수단(244)은 실제 키 값을 이용하여 허가된 사용자 여부를 인증하거나 금융거래 중계를 하는 것과 같은 후속 처리를 한다. 이 때 일례로 실제 키 값을 암호화하여 전송할 수 있다. 도어락과 같은 실시예에서는 상기 비공개 입력 장치 제어 수단(202)의 관리부에서 허가된 사용자 여부를 인증하여 도어를 개폐할 수 있다.

<52> 도 3은 키 디스플레이로서 범용 모니터를 사용하고 범용 컴퓨터로 제어를 수행하는 제2 실시예의 제어 구성도이다. 도시되어 있는 바와 같이, 퀀스 제어기와 그래픽 드라이버가 영상을 제어한다. 키패드로서 터치스크린을 사용할 수 있다. 비공개 입력 장치 제어 수단(202)은 보안 성능 제어부, 영상 배합 규칙 선정부, 암호화부, 관리부로 이루어지며, 디스플레이 보안 수준을 기준으로 영상 시퀀스 생성 수단(212), 셔터 개폐 시퀀스 및 셔터 개폐 신호 생성 수단(214), 비공개 영상 및 마스킹 영상 생성 수단(216)을 제어한다.

- <53> 모니터 정보 획득 수단(308)은 모니터(306)의 해상도, 리프레쉬 사이클 시간(refresh cycle time), 수직동기(vertical sync), 수평 동기(horizontal sync) 등의 정보를 읽어 비공개 입력 장치 제어 수단(202)에 제공한다.
- <54> 시퀀스 제어기(210)는 상기 비공개 입력 장치 제어 수단(202)과 정보를 교환하면서 생성된 영상 시퀀스에 따라 비공개 영상 및 마스킹 영상 생성 수단(216)에서 생성된 비공개 영상 및 마스킹 영상을 그래픽 드라이버(302)를 통하여 비디오 제어기(304)에 제공한다. 비디오 제어기(304)는 영상 시퀀스에 따라 키 영상의 비공개 영상 및 마스킹 영상을 모니터(306)에 디스플레이한다.
- <55> 또한 시퀀스 제어기(210)는 셔터 개폐 시퀀스 및 셔터 개폐 신호 생성 수단(214)에서 생성된 셔터 개폐 신호를 적절히 제어하여 P-S 송수신부(208)를 통하여 셔터 개폐 수단(108)에 전송한다.
- <56> 키패드 자판 배치 수단(220)은 결정된 현재 시점의 키 배치를 비공개 입력 장치 제어 수단(202)에 전송하고, 비공개 입력 장치 제어 수단(202)의 관리하에 시퀀스 제어기(210)와 비공개 영상 및 마스킹 영상 생성 수단(216)이 키 배치에 해당하는 영상을 비디오 제어기(304)를 통해 모니터(306)에 디스플레이한다. 사용자는 모니터(306)에 디스플레이된 키 배치를 비공개로 보면서 터치스크린과 같은 키패드(106)에서 정보를 입력한다. 키패드(106)에서 입력된 키는 키패드 제어기(206)에서 해당하는 위치 키 값으로 판독되고 판독된 위치 키 값이 키패드 자판 배치 수단(220)의 키 배치에 따라 실제 키 값으로 변환된다. 사용자가 입력한 실제 키 값은 비공개 입력 장치 제어 수단(202)의 관리부에서 처리된다. 입력 장치 제어 수단(202)에서 실제 키 값을 이용하여 허가된 사용자 여부를 인증하거나 금융거래 중계를 하는 것과 같은 후속 처리를 할 수 있다.

- <57> 도 4는 전용 드라이버를 사용하는 제3 실시예의 제어 구성도이다. 도 4에 도시된 제어 구성도는 전용 드라이버를 사용하는 것을 제외하고는 도 3과 동일하다. 본 실시예에서는 전용 드라이버와 그래픽 드라이버가 영상을 제어한다.
- <58> 전용 드라이버(410)는 생성된 영상 시퀀스에 따라 마스킹 영상 생성 수단(418)에서 생성된 마스킹 영상을 비디오 제어기(304)에 제공하거나 비디오 제어기(304)의 컬러 테이블을 실시간 변경 제어한다. 또한 전용 드라이버(410)는 생성된 영상 시퀀스에 따라 비디오 제어기(304)가 비공개 영상 메모리 블록과 마스킹 영상 메모리 블록을 스위칭하도록 함으로써 모니터(306)로의 영상 전송을 제어한다.
- <59> 그래픽카드와 같은 비디오 제어기(304)는 비디오 메모리를 구비하고 있으며, 그래픽 드라이버(302)로부터 받은 비공개 영상인 키 영상과 전용 드라이버(410)로부터 받은 키 영상의 마스킹 영상을 영상 시퀀스에 따라 모니터(306)에 디스플레이한다. 영상 시퀀스는 전용 드라이버에 의해 제공되고 제어된다.
- <60> 또한 전용 드라이버(410)는 셔터 개폐 시퀀스 및 셔터 개폐 신호 생성 수단(214)에서 생성된 셔터 개폐 신호를 적절히 제어하여 P-S 송수신부(208)를 통하여 셔터 개폐 수단(108)에 전송한다.
- <61> 도 5는 본 발명에 따른 비공개 정보 입력 시스템의 작동 순서도이다. 비공개 영상은 P, 마스킹 영상은 M, 중간상태 영상은 b로서 각각 표시한다. 중간상태 영상(b)은 비공개 영상(P)이나 마스킹 영상(M)이 아닌 영상의 총칭으로서 주로 비공개 영상(P)과 마스킹 영상(M)의 중간 형태의 영상으로 구성되어 사용자의 시각적 피로를 줄이고 보안성을 향상시키는 데 사용하며, 비공개 영상 및 마스킹 영상 생성 수단(216, 416, 418)으로부터 생성될 수 있다. 비공개 영상(P), 마스킹 영상(M), 중간상태 영상(b) 등으로 구성된 영상 시퀀스는 시퀀스에 중간상태 영상

(b)이 있던지 없던지 간략히 P/M 영상 시퀀스라 정의한다. 시스템 기본값으로 또는 오퍼레이터가 디폴트 디스플레이 보안 성능 수준을 설정한다(500). 디폴트 디스플레이 보안 성능 수준에 따라 디폴트 P/M 영상 배합 규칙을 선정하고 디폴트 P/M 영상 시퀀스와 디폴트 셔터 개폐 시퀀스를 생성한다(502). 또한 디폴트 셔터 개폐 시퀀스에 따라 현재 시점의 셔터 개폐 신호를 생성한다. 다음에는 디폴트 키 영상을 디스플레이하고 정보 입력 모드가 되어 사용자의 사용을 대기한다(504). 디폴트 정보 입력 모드는 비공개 정보 입력 모드일 수 있고, 일반 정보 입력 모드일 수 있다. 사용자가 비공개 정보 입력을 위해 비공개 키패드 입력 장치에서 패널 모양의 셔터 개폐 수단(108)을 들면 셔터 개폐 수단(108)의 사용 감지 수단에서 신호를 발생시켜 입력 장치 제어 시스템(102)에 전송한다(506). 입력 장치 제어 시스템(102)은 셔터 개폐 수단의 사용 감지 신호를 전송 받으면 비공개 입력 모드로 전환하여 비공개 키 배치를 하고(508), 설정된 영상 시퀀스에 따라 키 디스플레이(104)에 디스플레이한다(510). 다음 단계는 사용자가 현재의 디스플레이 보안 성능 수준을 변경할 지 여부를 선택한다(512). 변경을 선택하면 사용자는 원하는 디스플레이 보안 성능 수준을 선택한다(514). 다음에는 앞에서 선택된 디스플레이 보안 성능 수준에 따라 P/M 영상 배합 규칙을 선정하고 P/M 영상 시퀀스와 셔터 개폐 시퀀스를 생성한다(516). 또한 셔터 개폐 시퀀스에 따라 현재 시점의 셔터 개폐 신호를 생성한다. 다음에는 변경된 영상 시퀀스에 따라 키 영상을 디스플레이하고 정보 입력 모드가 되어 사용자의 정보 입력을 대기한다(518). 다음 단계에서는 사용

자가 키배치를 변경할 지 여부를 선택한다(520). 단계(520)에서 키 배치 변경을 선택하면 키 배치 유형을 변경하거나 키 배치를 변경하여(522), 키 디스플레이(104)에 디스플레이한다. 단계(520)에서 키 배치 변경을 선택하지 않으면 단계(524)로 간다. 단계(524)에서 사용자가 비공개로 정보를 입력하면 입력한 정보를 키 값으로 해독하고 후속 처리를 진행한다(526). 사용자가 정보를 입력한 후에 셔터 개폐 수단(108)을 놓으면 셔터 개폐 수단(108)의 사용 감지 수단에서 신호를 발생시켜 입력 장치 제어 시스템(102)에 전송한다. 신호를 받으면 디폴트 입력 모드로 전환하고 사용자 정보 입력을 종료한다(528).

<62> 도 6a 내지 도 6e는 본 발명에 따른 키패드 배치 방법을 설명하는 도면이다. 키 배치 유형에는 무작위 배치, 쉬프트(shift) 배치, 회전 배치 유형이 있다. 도 6a는 통상적인 배치 유형을, 도 6b는 무작위 배치 유형을 도시하고 있다. 무작위 배치를 하면 사용자가 키를 입력함에 있어서 불편하기 때문에 쉬프트 배치나 회전 배치를 쓸 수 있다. 도 6c는 두 가지 쉬프트 배치 예를 보여준다. 본 발명에 따른 쉬프트 배치의 일 예에서는 도 6c와 같이 키의 순서는 뒤바뀌지 않고 키의 위치만 특정한 방식으로 쉬프트된다. 도 6d는 일반적인 키패드를 이용한 사각 회전 배치의 예이다. 사각 회전 배치에서는 키의 순서는 뒤바뀌지 않고 시작점이 임의로 선정된다. 도 6e는 원형 키패드를 이용한 원형 회전 배치의 예이다. 원형 회전 배치에서는 키의 순서는 뒤바뀌지 않고 시작점이 임의로 선정된다.

<63> 도 7a 및 도 7b는 본 발명에 따른 완성형 혼합 영상을 설명하는 도면이다. 비공개 영상 및 마스킹 영상 생성 수단(216, 416, 418)으로부터 생성된 비공개 영

상 및 마스크 영상은 영상 시퀀스에 따라 디스플레이 장치(104)에 실시간으로 시간 순차적 혼합되어 보여지게 된다. 여기에서는 셔터 개폐 수단을 사용하지 않고 맨눈으로 보는 혼합 영상이 비공개 영상에 무관하게 특정한 의미를 갖는 단일한 영상으로 보일 때 이를 "완성형 혼합 영상"으로 정의한다. 또한 특정한 비공개 영상과 시간 순차적으로 혼합되어 상기 완성형 혼합 영상이 되도록 만드는 마스크 영상을 "완성형 마스크 영상"이라 정의한다. 일례로 비공개 영상이 3 일 때 완성형 마스크 영상으로서 도 7a와 같은 마스크 영상을 생성하고, 비공개 영상이 7 일 때 도 7b와 같은 마스크 영상을 생성하면 혼합 영상은 단일하게 8로 보인다. 마찬가지로 나머지 모든 숫자에 대해서도 적절한 완성형 마스크 영상을 선정하여 혼합하면 모두 8로 보이는 완성형 혼합 영상을 만들 수 있다.

<64> 도 8a 내지 도 8c는 본 발명에 따른 유사 완성형 혼합 영상을 설명하는 도면이다. 도 8에 도시된 완성형 혼합 영상과 유사하게 보이는 혼합 영상을 만드는 마스크 영상을 생성한다. 이와 같은 혼합 영상의 집합을 "유사 완성형 혼합 영상 집합"이라 정의하고, 유사 완성형 혼합 영상을 만드는 마스크 영상을 "유사 완성형 마스크 영상"이라 정의한다. 이 때는 하나의 비공개 영상에 대하여 다양한 유사 완성형 마스크 영상들을 만들 수 있다. 도 8은 7-세그먼트 LED 디스플레이를 가진 키패드의 실시예로서, 완성형 혼합 영상이 8이라면 유사 완성형 혼합 영상은 8과 유사한 영상으로서 8에서 일부분이 삭제되거나 8에 특정 획이 추가된 영상 등이 가능하다. 일례로 도 8에서와 같이 비공개 영상 3이 혼합 영상 9로 보이게 하거나, 비공개 영상 1이 혼합 영상으로서 좌우 바뀐 6 또는 3으로 보이게 할 수 있는 등 비공개 영상의 종류에 따라 여러 종류의 유사 완성형 혼합 영상을 만들 수 있는 유사 완성형 마스크 영상이 가능하다.

<65> 여기서는 7-세그먼트 LED 디스플레이를 구비한 키패드의 실시예를 중심으로 기술하였지만, 일반적인 범용 디스플레이를 구비한 키패드에서도 완성형 혼합 영상 방법과 유사 완성형

혼합 영상 방법이 적용될 수 있다. 범용 디스플레이 장치는 7-세그먼트 LED보다 많은 픽셀 수를 가지므로 다양한 폰트로 숫자 표현이 가능하다. 일 실시예에서는 범용 디스플레이를 구비한 키패드에서 7-세그먼트 LED 디스플레이를 구비한 키패드 경우와 동일한 폰트의 숫자 표현을 사용하여 디스플레이하고 입력한다. 다른 실시예에서는 7-세그먼트 LED에서 구현할 수 없는 다른 폰트의 숫자 표현을 사용한다. 이 때는 완성형 혼합 영상이 8과 같은 단순한 모양이 아니라 상기 폰트로 디스플레이 가능한 숫자들을 모두 겹친 복잡한 모양이 된다. 완성형 마스킹 영상은 비공개 영상에 해당하는 숫자 이외의 숫자들을 모두 겹친 모양으로 만들 수 있다. 이러한 방법으로 생성된 완성형 혼합 영상은 많은 숫자가 동시에 보여지기 때문에 염탐자가 맨눈으로 정확한 비공개 영상 숫자를 식별할 수 없다.

<66> 완성형 혼합 영상을 만들기 위해서 바람직한 실시예에서는 비공개 영상과 완성형 마스킹 영상이 시간적으로 거의 동일한 배합 비율로 디스플레이되도록 영상을 생성하여 정확한 완성형 혼합 영상이 보여질 수 있도록 한다. 다른 실시예에서는 비공개 영상과 완성형 마스킹 영상의 시간적 배합 비율을 상이하게 하여 영상을 생성한다. 비공개 영상과 완성형 마스킹 영상의 비율을 다르게 배합하면 영상의 대비(contrast)가 약간 불균일한 부분이 발생하여 완성형 혼합 영상이 마치 유사 완성형 혼합 영상처럼 보여지도록 할 수 있다. 이런 경우라도 영상배합 규칙에 따라 영상 시퀀스가 시간에 따라 가변하면 비공개 입력 장치의 디스플레이 보안 성능이 저하되지는 않는다.

<67> 도 9a 내지 도 9f는 본 발명에 따른 완성형 혼합 영상을 이용한 영상 배합 규칙, 영상 시퀀스, 셔터 개폐 시퀀스 선정을 설명하는 도면이다. 비공개 영상(숫자 5)에 대한 마스킹 영상 및 중간상태 영상이 도시되어 있다. 비공개 영상(도 9a) 및 마스킹 영상(도 9b)을 가지고 도 9d와 도 9e와 같이 주기 영상 시퀀스 및 비주기 영상 시퀀스를 각각 구현할 수 있다. 도 9f

는 중간상태 영상(도 9c)을 포함한 영상 시퀀스를 디스플레이한 예시이고 중간상태 영상은 전술한 바와 같이 비공개 영상의 일부로 구성될 수 있다. 완성형 혼합 영상을 만들기 위해서 바람직하게는 비공개 영상 및 완성형 마스킹 영상이 시간적으로 거의 동일한 비율로 배합될 수 있다. 다른 실시예에서는 비공개 영상과 완성형 마스킹 영상의 비율을 다르게 배합하여 혼합 영상이 유사 완성형 혼합 영상처럼 보여지도록 할 수 있다. 비공개 영상(도 9a)과 완성형 마스킹 영상(도 9b)의 배합비율과 같은 배합 규칙이 정해지면 이에 따라 영상 시퀀스를 생성한다. 일 실시예로서 도 9d와 같이 사용자의 시각 피로를 줄이기 위해서 비공개 영상과 완성형 마스킹 영상이 주기적으로 반복되어 보여지도록 영상 시퀀스를 설정할 수 있다. 다른 실시예로서 도 9d와 같이 비공개 영상과 완성형 마스킹 영상이 전체적으로 특정한 규칙을 갖는 비주기적인 시퀀스 형식으로 보여지도록 영상 시퀀스를 설정할 수 있다.

<68> 본 발명의 일 실시예에서는 비공개 영상과 마스킹 영상의 중간인 중간상태 영상(도 9c)을 생성하여 특정한 영상 시퀀스와 함께 디스플레이할 수 있다. 본 발명에서는 비공개 영상(P), 마스킹 영상(M), 중간상태 영상(b)으로서 각각의 영상을 표시한다. 일례로서 도 9d와 같은 주기 영상 시퀀스, 도 9e와 같은 비주기 영상 시퀀스 (PPMPMMPMMP), 도 9f와 같은 중간상태 영상을 포함한 시퀀스 (PBMPMBPBMP)를 생성할 수 있다. 중간상태 영상을 포함하여 영상 시퀀스를 생성할 시에는 바람직한 실시예로서 영상의 각 부분의 시간 평균 빈도가 균일하게 되도록 설정한다.

<69> 셔터 개폐 시퀀스는 2-상태 셔터 개폐 또는 중간상태 셔터 개폐를 포함한 셔터 개폐 상태 시퀀스로 구현될 수 있다. 2-상태 셔터 개폐는 비공개 영상시 셔터를 최대로 열고 마스킹 영상시 셔터를 최대로 닫는 단순한 동작을 하게 된다. 2-상태 셔터 개폐 실시예에서 셔터 개폐 시퀀스가 비주기적이면 셔터가 열리고 닫히는 주기가 일정치 않아 사용자의 눈에 많은 피로를

유발할 수 있다. 중간상태 셔터 개폐를 포함한 셔터 개폐에서는 열림과 닫힘 상태 외에 적어도 하나 이상의 중간상태를 포함하여 셔터 개폐를 한다. 본 발명의 일 실시예에서는 셔터의 개폐 상태가 연속적으로 이어질 때 셔터를 중간상태로 개폐하고 영상도 이에 상응하도록 조작하여 불규칙한 셔터의 개폐로 인한 눈의 피로를 효과적으로 줄일 수 있다.

<70> 중간상태 영상을 디스플레이 할 때, 일 실시예에서는 중간상태 셔터 개폐를 할 수 있고 다른 실시예에서는 닫힘 또는 열림 상태로 셔터 개폐를 할 수 있다. 다른 실시예에서는 비공개 영상이나 마스킹 영상을 디스플레이할 때 중간상태 셔터 개폐를 할 수 있다. 중간상태 영상을 디스플레이 할 때 중간상태 셔터 개폐를 하면 비공개 영상과 마스킹 영상의 교체가 부드럽도록 유도할 수 있고 중간상태 셔터 개폐시 눈에 맺히는 영상으로 인한 비공개 영상의 인식을 저하를 막을 수 있다. 일 실시예로서 중간상태 셔터 개폐시 영상은 도 9에서와 같이 비공개 영상의 일부 혹은 전부를 보여주어 비공개 영상의 인식을 높일 수 있다.

<71> 유사 완성형 혼합 영상을 이용한 영상배합 규칙, 영상 시퀀스, 셔터 개폐 시퀀스 선정은 상기 완성형 혼합 영상을 이용한 일 실시예로서의 도 9를 참조하여 쉽게 적용할 수 있다.

<72> 도 10a 내지 도 10f는 본 발명에 따른 완성형 혼합 영상을 이용한 요소 영상법을 설명하는 도면이다. 도 7과 같은 완성형 혼합 영상을 이용하는 경우, 염탐자가 허가받지 않은 다른 셔터 개폐 수단으로 엿보거나 고속 카메라로 연속 촬영하면 어느 순간 숨기고자 하는 숫자배치가 노출될 수 있다. 이러한 상황을 방지하기위해 본 발명의 일 실시예에서는, 각 숫자에 대한 비공개 영상과 완성형 마스킹 영상을 각 요소로 분할하여 이를 시간 순차적으로 배합하여 디스플레이한다. 마찬가지로 중간상태 영상도 분할요소로 나눌 수 있다. 이러한 방법을 이하 "요소 영상법"이라 칭하고 비공개 영상의 분할된 요소를 "비공개 영상 요소"라하고 마스킹 영상과 중간상태 영상의 경우 각각 "마스킹 영상 요소", "중간상태 영상 요소"라 칭한다. 요소 영상법

에서 영상 요소의 분할은 다수의 방법이 존재할 수 있고 다수의 분할 방법을 동시에 적용하여 영상 시퀀스를 구성할 수 있다. 요소 영상법은 요소 분할 방법 및 영상 요소 시퀀스가 임의로 변할 수 있어 염탐자는 허가받지 않은 셔터 개폐 수단이나 고속 카메라 촬영을 통해서 비공개 영상 요소 또는 마스킹 영상 요소만 볼 수 있으므로 의미있는 비공개 영상을 유추할 수 없게 된다.

<73> 완성형 혼합 영상을 만들기 위해서 바람직하게는 비공개 영상 요소 및 완성형 마스킹 영상 요소가 시간적으로 거의 동일한 비율로 배합될 수 있다. 다른 실시예에서는 비공개 영상 요소와 완성형 마스킹 영상 요소의 비율을 다르게 배합하여 혼합 영상이 유사 완성형 혼합 영상 처럼 보여지도록 할 수 있다. 요소 영상법을 사용하면 허가된 셔터를 통해 일정시간 이상 연속적인 비공개 영상 요소들을 시청해야 정확한 비공개 영상을 볼 수 있다.

<74> 요소 영상법에서 비공개 영상 요소 및 마스킹 영상 요소의 시퀀스는 일례로 도 10d와 같이 주기적으로 설정될 수 있다. 비공개 영상 요소 및 마스킹 영상 요소의 시퀀스를 도 10e와 같이 비주기 시퀀스로 생성하면 외부에서 허가되지 않은 셔터를 착용한 염탐자로부터의 보안성이 크게 향상된다. 비공개 영상 요소 및 마스킹 영상 요소의 시퀀스를 비주기 시퀀스로 할 때 사용자의 눈의 피로가 증가되지만, 도 10f와 같이 중간상태 영상 요소를 포함한 영상 시퀀스로 디스플레이하고 중간상태 셔터 개폐를 이용하면 피로를 감소시키면서 염탐자로부터의 보안성을 향상시킬 수 있다.

<75> 일 실시예로서 도 10은 숫자 5에 대한 요소 영상법의 예를 보여준다. 비공개 영상 요소, 마스킹 영상 요소와 중간상태 영상 요소는 도 10a 내지 도 10c에 도시되어 있는 바와 같이 분할될 수 있고, 주기적 영상 요소 시퀀스나 비주기적 영상 요소 시퀀스로 디스플레이 되면 사용자는 비공개 영상 요소의 시간 적분된 값으로 비공개 영상을 종합하여 볼 수 있게 된다.

일 실시예로서 도 10에서 숫자 5에 대한 비공개 영상 요소 분할은 P-1이나 P-2와 같이 다양한 방법으로 구성될 수 있다. 동일한 방법으로 마스킹 영상 요소 및 중간상태 영상 요소의 분할도 다수의 예가 존재할 수 있고 도 10에서는 한가지의 구성 예만 도시하였다. 일 실시예로서 도 10d 내지 도 10f에 도시되어 있는 바와 같이 두 가지 비공개 영상 요소(P-1, P-2)를 섞어서 디스플레이할 수 있다. 도 10f 분할된 중간상태 영상 요소를 포함한 영상 시퀀스 예이다.

<76> 유사 완성형 혼합 영상을 이용한 요소 영상법은 상기 완성형 혼합 영상을 이용한 요소 영상법으로부터 쉽게 유도하여 실시할 수 있다.

<77> 도 11a 내지 도 11c는 본 발명에 따른 동일 손동작 키 관리 방법을 설명하는 도면이다.

본 발명의 일 실시예에서는 동일 손동작 키 개념에 근거한 관리 방법을 제시한다. "동일 손동작 키"란 키패드를 가변 배치할 경우에 각각의 경우마다 동일한 손동작으로 입력을 해야 하는 키들의 쌍을 의미한다. 예를 들어, 시계방향 사각 회전 배치법을 사용하는 키패드일 경우에 도 11에서 도시한 바와 같이 비공개 영상을 여러 가지 형태로 배치할 수 있다. 도 11a와 같은 비공개 영상 배치 상태에서 비밀번호 '6927' 네자리를 모두 입력하는 경우라면, 그림과 같이 화살표로 표시한 네 키를 순차적으로 입력하게 된다. 이 때 동일 손동작 키는 도 11b의 경우 '4705', 도 11c의 경우 '5816'가 된다. 본 발명에서는, 시계방향 사각 회전 배치 키패드일 때 '6927', '4705', '5816' 등이 동일 손동작 키로서 관리된다. 염탐자가 사용자의 손동작을 정확히 염탐하였다면 '6927', '4705', '5816' 등을 가능한 비밀번호 후보로서 알게 되고, 염탐자는 상기 가능한 비밀번호 후보를 모두 입력하여 정확한 비밀번호를 알아내려고 할 것이다.

<78> 본 발명에서는 보안성을 더욱 향상시키기 위하여 비밀번호 등의 키 값이 입력되어야 할 때 옳은 키 값 대신 동일 손동작 키가 입력되면 부정 사용 신호로 판단하여 관리한다. 도 12는 동일 손동작 키 입력 관리 방법의 순서도이다.

<79> 먼저 키 영상을 디스플레이하고 비공개 정보 입력 모드가 되어 사용자의 사용을 대기한다(1200). 단계(1202)에서 사용자가 정보를 입력하면 입력한 정보를 키 값으로 해독한다(1204). 다음 단계에서는 사용자가 입력한 키 값이 옳은 키 값인지 판단한다(1206). 옳은 키 값이라면 정당한 사용자임을 인증하고 후속 처리를 하고(1208) 사용자 정보 입력을 종료한다(1210). 단계(1206)에서 옳은 키 값이 아니라면 단계(1212)에서 입력한 키 값이 옳은 키 값의 동일 손동작 키 값 가운데 하나인지를 판단한다. 입력한 키 값이 옳은 키 값의 동일 손동작 키 값이 아니라면 단계(1200)로 가서 사용자의 재 입력을 대기한다. 입력한 키 값이 옳은 키 값의 동일 손동작 키 값이라면 사용자의 키 입력 손동작을 염탐한 부정 사용자일 가능성이 크므로 부정 사용 처리를 한다(1214). 부정 사용 처리에는 해당 카드 사용을 일시적으로 정지시키거나, 사용자에게 부정 사용을 알리는 휴대전화 문자 메시지를 전송하는 방법 등이 있다.

<80> 다른 실시예에서는 동일 손동작 키가 누적하여 특정 횟수 이상 입력될 때만 부정 사용 처리를 할 수 있다.

<81> 본 발명은 숫자키 실시예를 중심으로 기술하였지만 본 발명의 사상은 큰 변경없이 문자 키에도 동일하게 적용할 수 있다. 본 발명의 일 실시예에서는 휴대폰 키패드처럼 하나의 키에 숫자키와 문자키가 다중으로 할당된 키패드에서, 키가 가변 배치됨에 따라 숫자키 뿐만 아니라 문자키도 가변 배치되어 비공개로 디스플레이되고 정보 입력을 할 수 있다. 이에 따라 문자도 숫자와 마찬가지로 본 발명의 방법을 적용하여 보안성이 확보되는 상태에서 입력할 수 있다.

【발명의 효과】

<82> 이러한 본 발명에 의하여 사용자의 정보 입력 행위 과정을 총체적인 물리적 보안 측면에서 고려하여 안전한 비공개 정보 입력 장치 및 방법을 제공할 수 있다. 또한 사용자가 정보 입력을 할 때의 키패드의 자판 배치와 입력키를 염탐자가 엿보아 해독하는 것을 방지할 수 있다.

또한 사용자가 정보 입력을 할 때의 손동작을 염탐자가 엿보아 해독하는 것을 방지할 수 있다. 또한 키입력 수단 위에 있는 손자국이나 지문, 키패드 마모 등의 입력 흔적을 염탐자가 채취하여 사용자의 입력정보를 해독하는 것을 방지할 수 있다. 또한 비공개 정보 입력 시스템에 적합한 마스킹 영상을 생성할 수 있다. 또한 염탐자가 동일한 종류의 다른 셔터 개폐 수단을 가지고 엿보려 해도 정보 입력 내용을 알아챌 수 없도록 하는 비공개 정보 입력 장치 및 방법을 제공할 수 있다.

【특허청구범위】

【청구항 1】

옛보기를 통한 정보 유출을 방지하는 비공개 정보 입력 시스템에 있어서,
키 영상을 생성하는 수단과,
상기 키 영상을 마스킹하는 마스킹 영상을 생성하는 수단과,
상기 키 영상과 상기 마스킹 영상에 대한 영상 시퀀스를 생성하는 수단과,
상기 영상 시퀀스에 따라 상기 키 영상과 상기 마스킹 영상을 디스플레이하는 키 표시부와,
상기 키 표시부에 의해 디스플레이되는 키 영상의 소정 위치에서 상응하는 키의 정보를 입력받는 키 입력부와,
상기 키 입력부를 통해 입력된 정보를 상기 키 영상에 따라 실제 키 값으로 변환하는 비공개 입력 장치 제어수단을
포함하는 것을 특징으로 하는 비공개 정보 입력 시스템.

【청구항 2】

제 1 항에 있어서,
상기 키 영상을 생성하는 수단은 키 배치가 가변되는 키 영상을 생성하는 것을 특징으로 하는 비공개 정보 입력 시스템.

【청구항 3】

제 1 항에 있어서,

셔터부와, 상기 영상 시퀀스에 상응하는 셔터 개폐 시퀀스에 따라 상기 셔터부를 개폐하는 셔터 제어부를 구비하는 셔터 개폐 수단을 더 포함하는 것을 특징으로 하는 비공개 정보 입력 시스템.

【청구항 4】

제 3 항에 있어서,

상기 셔터 개폐 수단은 사용자의 사용 여부를 감지하여 상기 비공개 입력 장치 제어수단에 알리는 사용 감지 수단을 더 구비하는 것을 특징으로 하는 비공개 정보 입력 시스템.

【청구항 5】

제 1 항에 있어서,

상기 키 표시부 전면부에 부착된 주변광 차단 필터를 더 구비하는 것을 특징으로 하는 비공개 정보 입력 시스템.

【청구항 6】

제 1 항에 있어서,

정당 사용자 여부를 판정하는 사용자 인증부를 더 포함하는 것을 특징으로 하는 비공개 정보 입력 시스템.

【청구항 7】

제 1 항에 있어서,

상기 키 영상 생성 수단은 키 배치 유형을 결정하고, 상기 결정된 키 배치 유형을 갖는 하나의 키 배치를 랜덤하게 선택함으로써 현재 시점의 키 영상을 생성하는 것을 특징으로 하는 비공개 정보 입력 시스템.

【청구항 8】

제 1 항에 있어서,

상기 마스킹 영상은 상기 키 영상과의 혼합 영상이 맨눈으로 볼 때 상기 키 영상과 무관한 특정 의미를 갖도록 하는 것을 특징으로 하는 비공개 정보 입력 시스템.

【청구항 9】

제 8 항에 있어서,

상기 키 표시부는 키 표시 단위가 발광 다이오드에 의해 구성된 것을 특징으로 하는 비공개 정보 입력 시스템.

【청구항 10】

제 8 항에 있어서,

상기 키 표시부는 키 표시 단위가 7-세그먼트 발광 다이오드에 의해 구성되고, 상기 마스킹 영상은 상기 키 영상과의 혼합 영상이 맨눈으로 볼 때 8로 보이도록 하는 것을 특징으로 하는 비공개 정보 입력 시스템.

【청구항 11】

제 1 항에 있어서,

상기 마스킹 영상은 상기 키 영상에 해당하는 숫자 이외의 숫자를 모두 겹친 모양인 것을 특징으로 하는 비공개 정보 입력 시스템.

【청구항 12】

제 1 항에 있어서,

상기 키 영상은 배합될 때 소정 숫자를 표시하는 2 이상의 요소 영상으로 구성되는 것을 특징으로 하는 비공개 정보 입력 시스템.

【청구항 13】

제 1 항에 있어서,

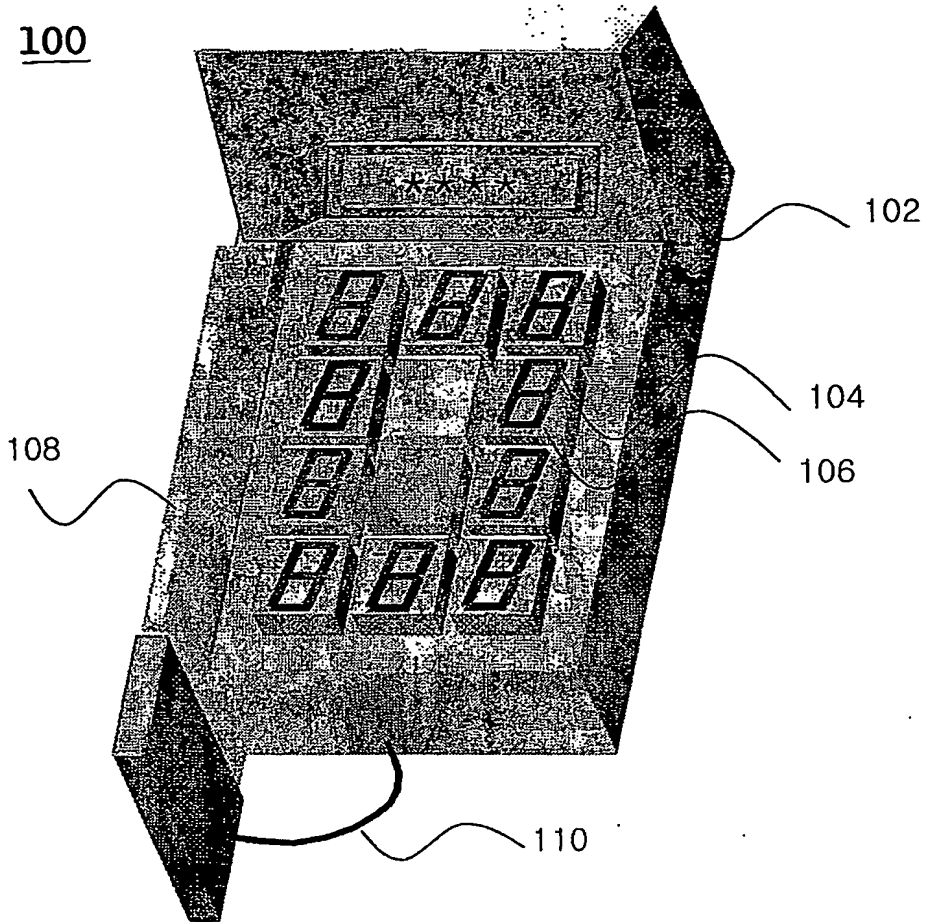
상기 키 영상과 상기 마스킹 영상의 중간 상태 영상을 생성하는 수단을 더 포함하며,

상기 영상 시퀀스 생성 수단은 상기 키 영상과 상기 마스킹 영상과 상기 중간 상태 영상에 대한 영상 시퀀스를 생성하고, 상기 키 표시부는 상기 영상 시퀀스에 따라 상기 키 영상과 상기 마스킹 영상과 상기 중간 상태 영상을 디스플레이 하는 것을 특징으로 하는 비공개 정보 입력 시스템.

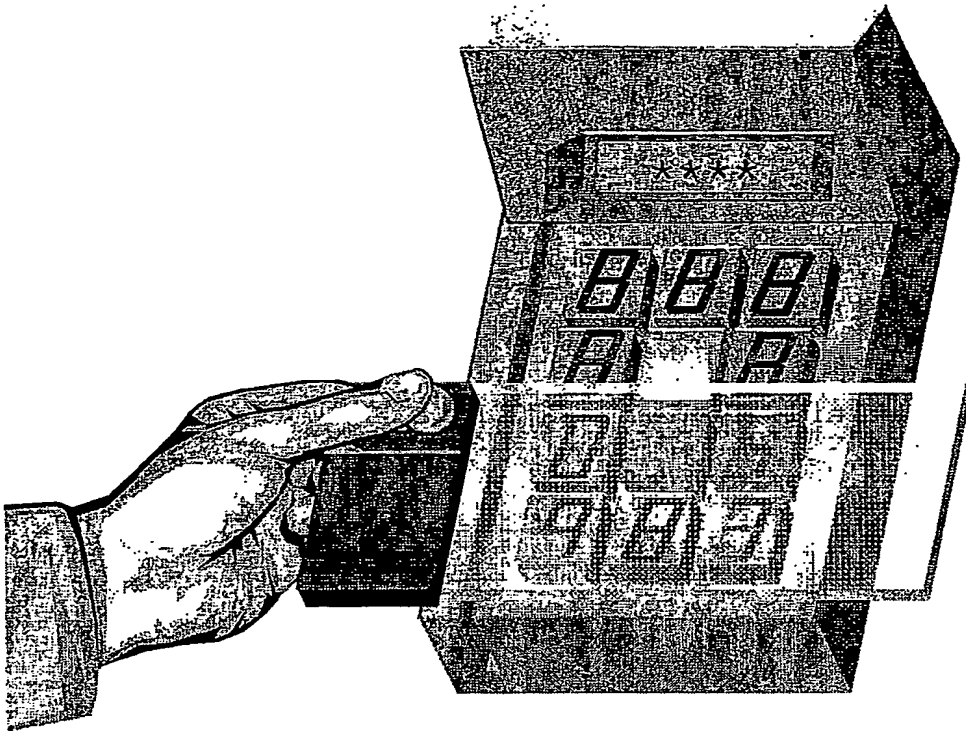
【도면】

【도 1a】

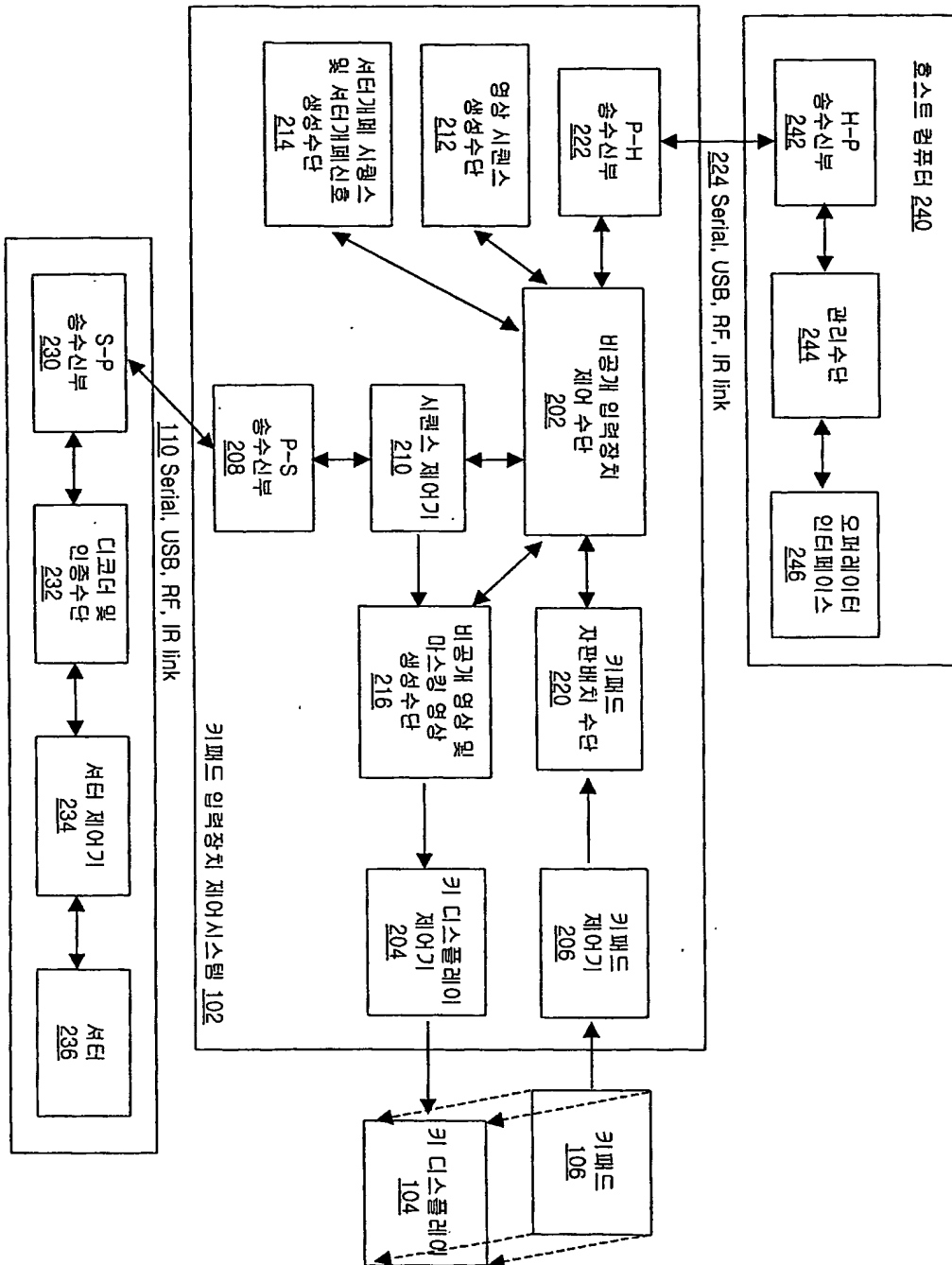
100



【도 1b】

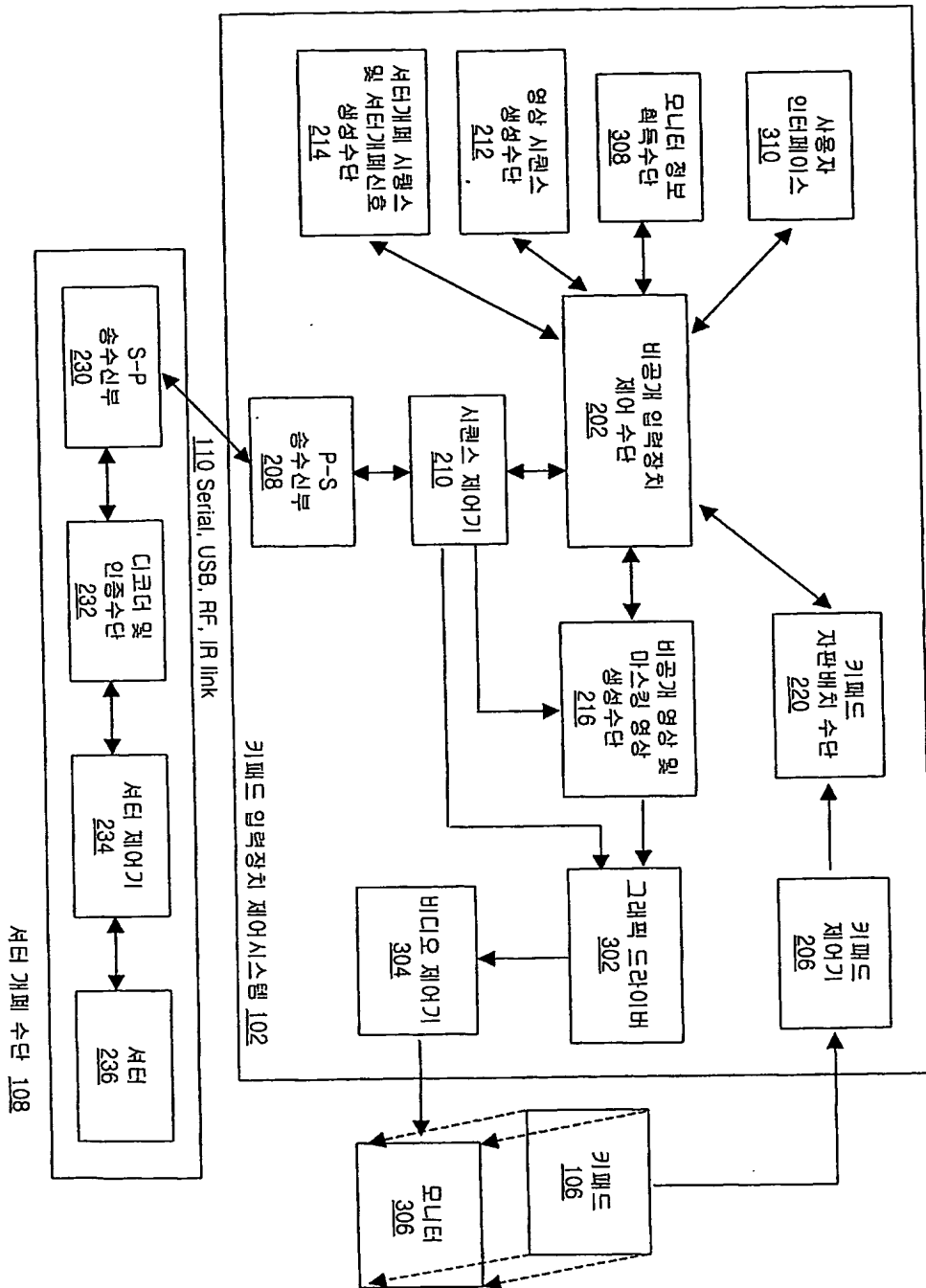


【도 2】

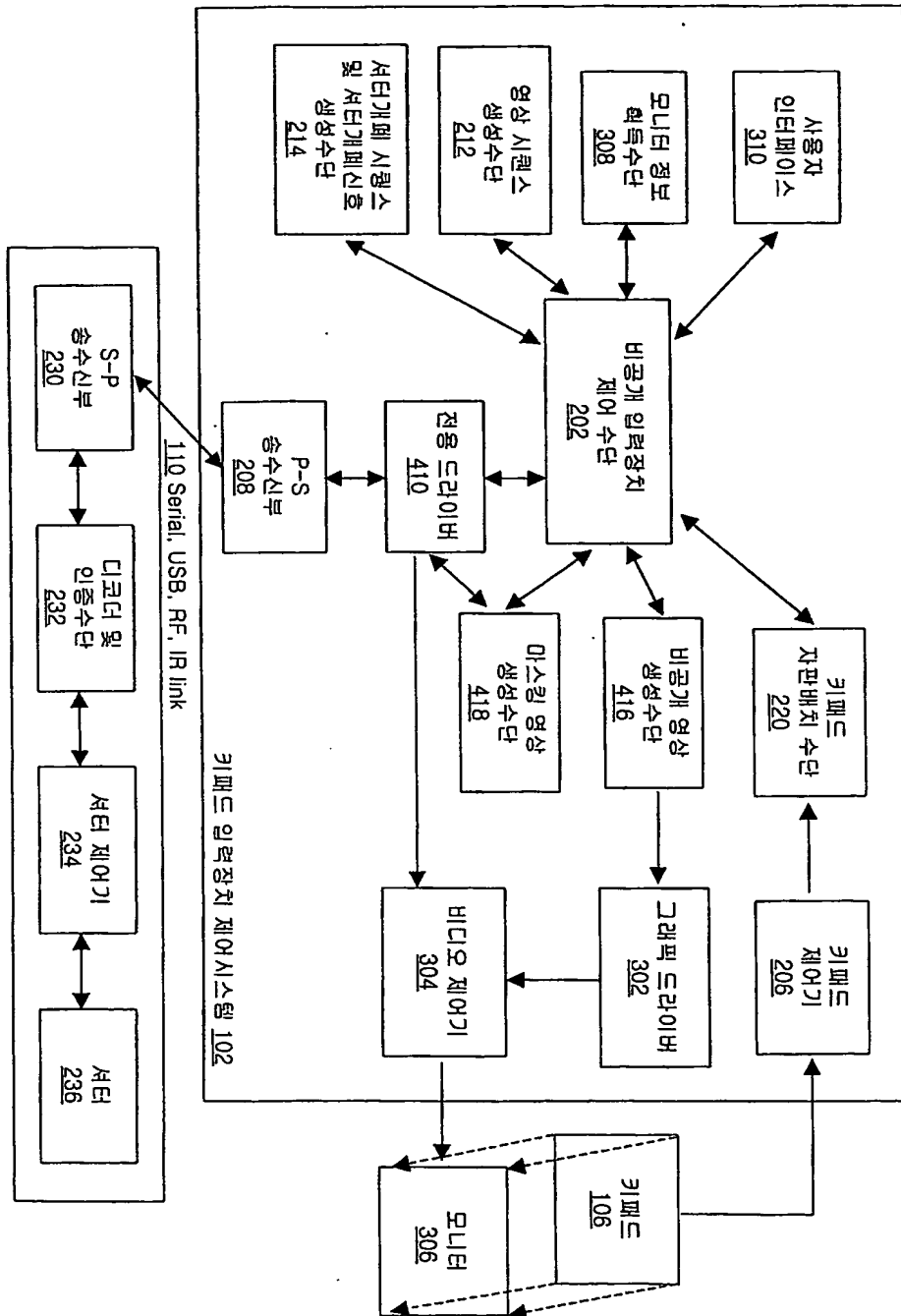


키프레임 캡처수단 108

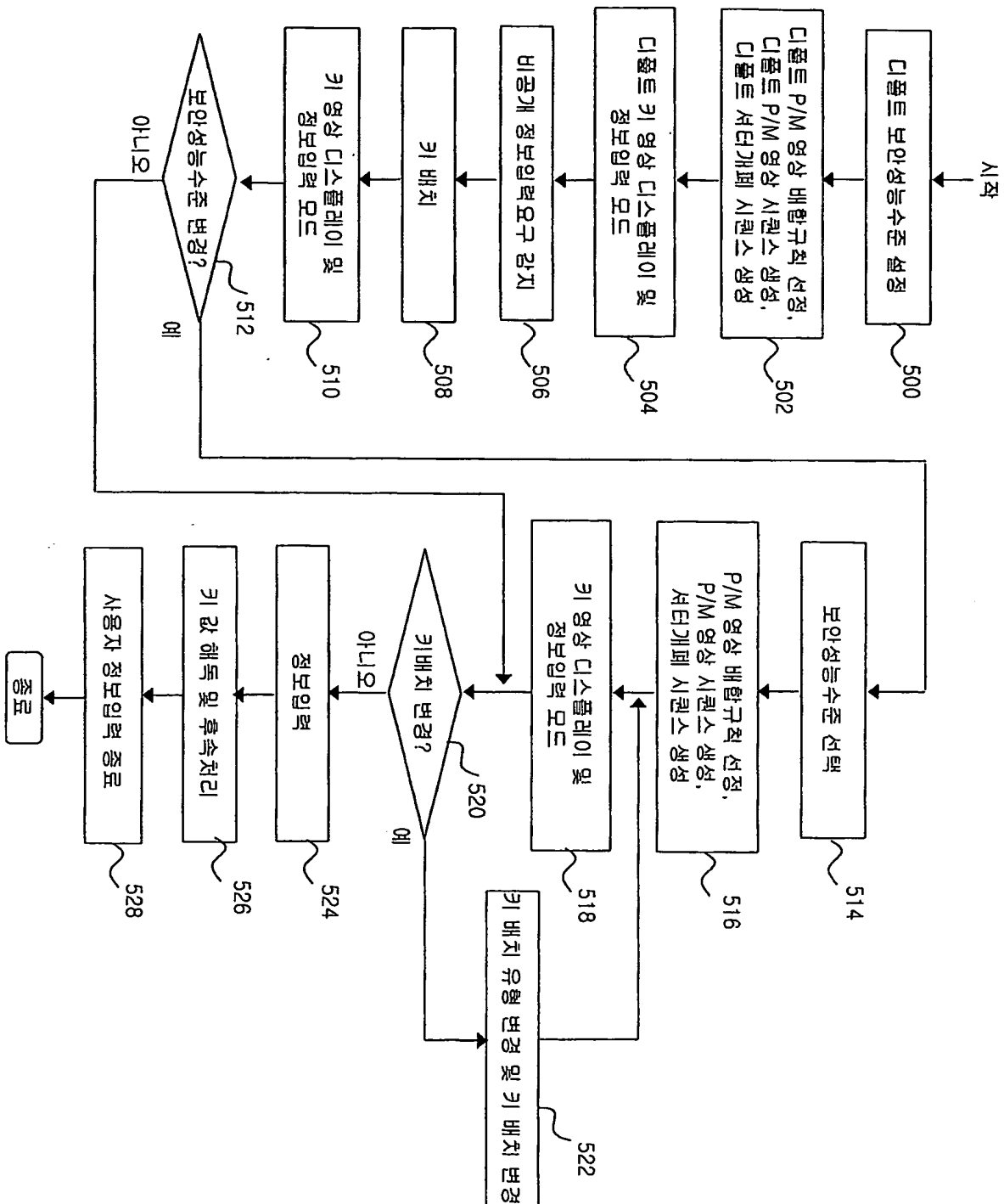
【도 3】



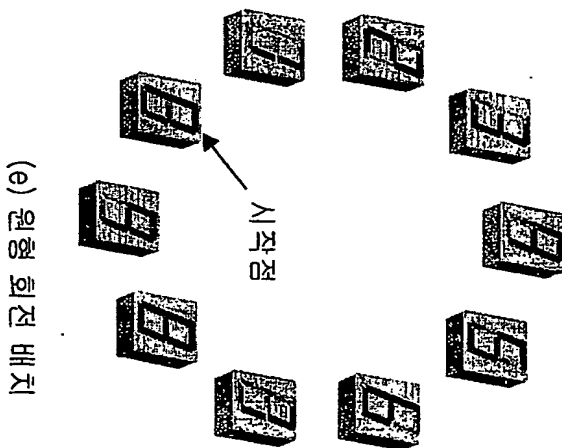
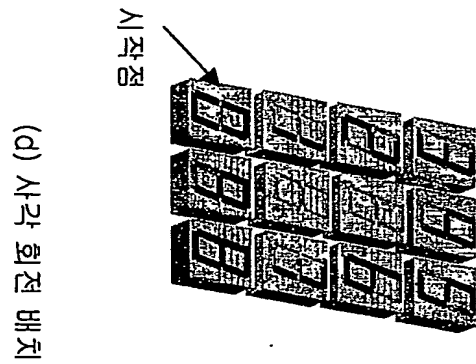
【도 4】



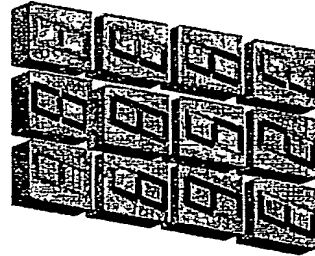
【도 5】



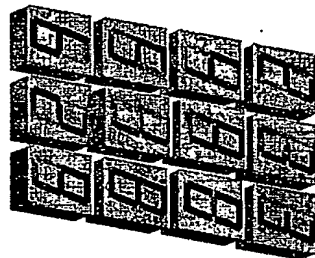
【도 6】



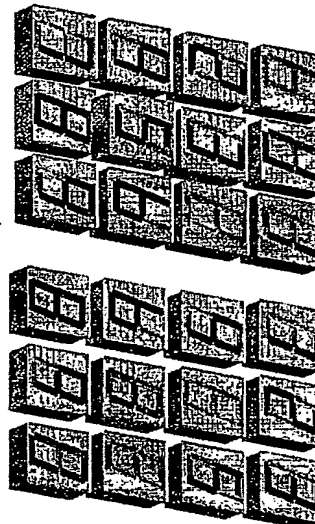
(a) 일반 배치



(b) 무작위 배치



(c) Shift 배치



【도 7】

$$8 + 8 = 8$$

(a) 예시1

$$8 + 8 = 8$$

(b) 예시2

【도 8】

$$8 + 8 = 8$$

(a) 예시1

$$8 + 8 = 8$$

(b) 예시2

$$8 + 8 = 8$$

(c) 예시3

【도 9】



P

(a)



M

(b)



B



(c)



P



M



P



M



P



M



P



M



P



M

(d)



P



P



M



P



M



M



P



M



M



P

(e)



P



B



M



P



M



B



P



B



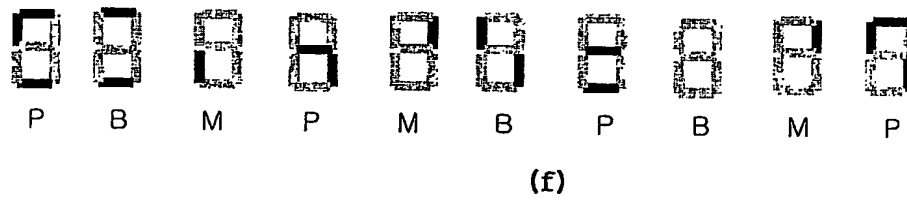
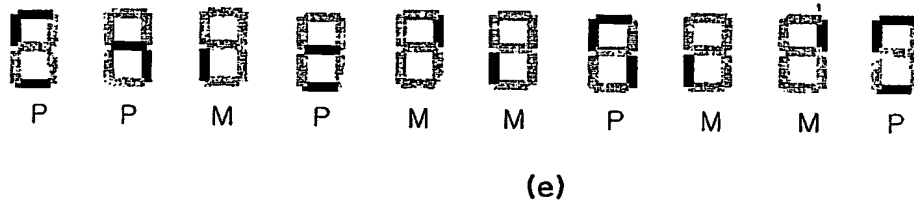
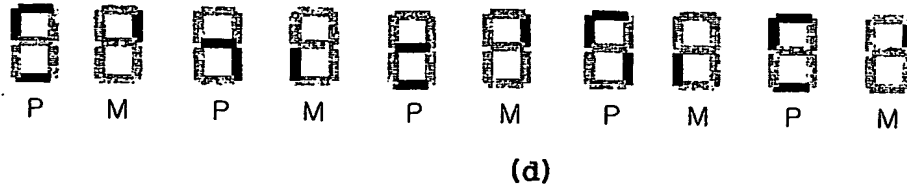
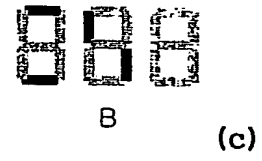
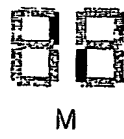
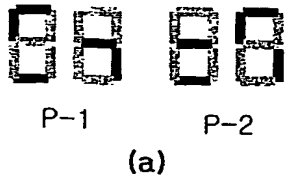
M



P

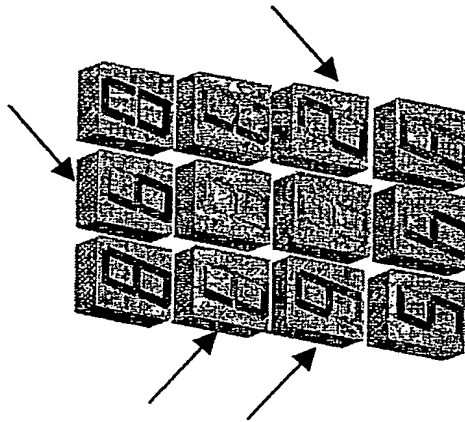
(f)

【도 10】

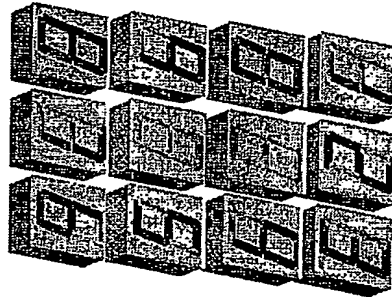


【도 11】

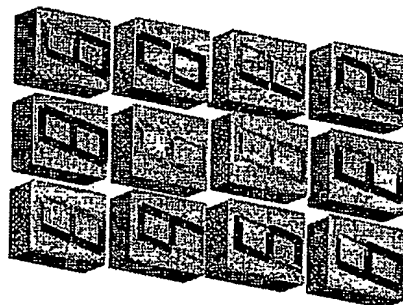
(a)



(b)



(c)



【도 12】

